Sci Eng Ethics (2014) 20:701–715
DOI 10.1007/s11948-014-9551-y

ORIGINAL PAPER

Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities

Myriam Dunn Cavelty

Received: 21 November 2013 / Accepted: 13 April 2014 / Published online: 30 April 2014

Abstract Current approaches to cyber-security are not working. Rather than producing more security, we seem to be facing less and less. The reason for this is a multi-dimensional and multi-faceted security dilemma that extends beyond the state and its interaction with other states. It will be shown how the focus on the state and "its" security crowds out consideration for the security of the individual citizen, with detrimental effects on the security of the whole system. The threat arising from cyberspace to (national) security is presented as possible disruption to a specific way of life, one building on information technologies and critical functions of infrastructures, with relatively little consideration for humans directly. This non-focus on people makes it easier for state actors to militarize cyber-security and (re-)assert their power in cyberspace, thereby overriding the different security needs of human beings in that space. Paradoxically, the use of cyberspace as a tool for national security, both in the dimension of war fighting and the dimension of mass-surveillance, has detrimental effects on the level of cyber-security globally. A solution out of this dilemma is a cyber-security policy that is decidedly anti-vulnerability and at the same time based on strong considerations for privacy and data protection. Such a security would have to be informed by an ethics of the infosphere that is based on the dignity of information related to human beings.

Keywords Cyber-security · Human security · Surveillance · Information ethics

M. Dunn Cavelty (✉)
Center for Security Studies (CSS), ETH Zurich, Haldeneggsteig 4, IFW (C 25.1), 8092 Zurich, Switzerland
e-mail: dunn@sipo.gess.ethz.ch

Introduction

Cyber-threats and the measures necessary to counter them are the security issue of the hour. In recent years, a number of sophisticated cyber-attacks and intensifying media attention have combined to give the impression that cyber-incidents are becoming more frequent, more organised, more costly, and altogether more dangerous. As a result, cyber-fears have percolated upwards, from the expert level to executive decision-makers and politicians; and diffused horizontally, advancing from mainly being an issue of relevance to the US to one that is at the top of the threat list of more and more countries, resulting in a flurry of government-led and private-led cyber-security initiatives.[1]

However, despite concerted efforts and increasing sums of money spent on various aspects of cyber-security over the years, cyberspace does not seem to become more secure—rather the opposite, considering the plethora of technical and governmental reports that use the language of urgency and general doom. Furthermore, the actions of some states convey an additional level of unease: Though consolidated numbers are hard to come by, the amount of money spent on defence-related aspects of cyber security is rising (Brito and Watkins 2011; Boulanin 2013). Furthermore, an increasing number of states go (semi) public about opening up 'cyber-commands', which are military units for (potentially offensive) cyber war activities.

If we assume that more—rather than less—security in and through cyberspace is one, if not the key goal of cyber-security policies, then the current approach to cyber-security is not working. Worse, as I will show in this article, actions geared towards gaining more security are (directly and indirectly) to blame for making both the virtual but also, by implication, the real world *less* and not more secure. What we seem to be facing is a "security dilemma", where efforts by one actor (traditionally, states) to enhance its security decrease the security of others (Jervis 1978). Because cyber-capabilities cannot easily be divulged by normal intelligence gathering activities, uncertainty and mistrust are on the rise. Although most states still predominantly focus on cyber-defence issues, measures taken by some nations are seen by others as covert signs of aggression by others and will likely fuel more efforts to master "cyber-weapons" worldwide (Dunn Cavelty 2012; Rueter 2011).

That said, the cyber-security dilemma, like other security dilemmas before it, extends to much more than just the security of and between states. In its basic form, cyber-security signifies a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. The related security discourse is about a diverse set of threat forms, ranging from basic computer viruses to cyber-crime and cyber-espionage activities, as well as cyber-terror and cyber-war. Each sub-issue is represented and treated in a distinct way in the political process: Multiple actors employ different political, private, societal, and corporate notions of security to mobilise (or de-mobilise) different audiences (Stevens and Betz 2013; Dunn Cavelty 2008). In a less

[1] Several governments have released or updated cyber-security or cyber-defense strategies in the last several years. See http://www.ccdcoe.org/328.html for a good overview.

basic form, then, cyber-security is a heterogeneous set of discourses and practices with multiple, often contradictory effects. Because cyberspace is a realm used and colonized by many different actors for a variety of things, the security-actions by states also directly come to bear on human lives in multiple ways—and vice versa.

In this article, I want to propose possible avenues for breaking the cyber-security-dilemma, especially since the basics of the situation are malleable by human action: Cyberspace, unlike the air, space, or the sea, is an entirely man-made realm, at all times shaped by economic and political forces (Deibert et al. 2008). In the pages that follow, I will first analyse the cyber-security dilemma by focusing on the way the issue is talked about and approached on the policy level and then by looking at how the social entities with power (mainly states and big corporations) shape this discourse and the (physical) information environment by specific security-related practices. In general, it will be shown how the focus on the state and "its" security crowds out consideration for the security of the individual citizen. In other words, the type of security that is currently produced is often *not* security relevant to the people. That way, a problem for human security is created (Axworthy 2001), which consists of a sustained feeling of insecurity, insecurities in the form of (material) vulnerabilities in the infosphere, and exploitation of these insecurities by several political actors.

The diagnosis of how the dilemma is created in parts one and two will then allow me to suggest a remedy in the third part. I argue that national security and a form of security that "distances itself from the exclusive grip of a state-determined concept and becomes security relevant to people" (Hoogensen and Stuvøy 2006: 219) should not be and must not be at loggerheads with each other. In cyber-security in particular, the two can meet. If we want national security and human security at the same time, we need a type of security that is based on strong considerations for privacy and data protection and is decidedly anti-vulnerability. Such a security, which I outline in the last chapter, should be informed by a human-centric information ethics of the infosphere (Floridi 1999; Capurro 2006).

What Kind of Security is Cyber-Security?

In this chapter, I will introduce the specificities of the cyber-security relevant discourse in order to show what kind of security cyber-security is.[2] I trace two elements: the specificities of the "threat" and the related "referent object" (that which is seen in need of protection). In any political process, the definition of referent objects is not only closely connected to how a danger is viewed, it also is an unavoidable decision since any danger discourse must be tied to some kind of endangered entity to become meaningful (Hagmann and Dunn Cavelty 2012). What is shown in this chapter is that the "human" is presented as a direct threat in the form of the (evil) hacker, the inadequate software developer or system

[2] A focus on discursive expressions should not be understood as a denial that there are "real world" issues at stake. The reality of network incidents is undisputed; however, the analysis goes explicitly beyond the impacts of "real" (objective) threats arising from cyberspace to look at their representation in the political process.

administrator, but is hardly ever a specific and direct referent object of security. The threat to (national) security is presented as possible disruption to a specific way of life—one building on information technologies, economic performance and "critical" functions of infrastructures—but the direct threat to human security, especially a threat that undermines acquired values such as anonymity, privacy, freedom of speech, free access to information, etc. does not figure prominently in the policy discourse.

An Amorphous Threat and its Representation

In the mid-1990s, a growing concern with information security found a technical vocabulary, a set of analytical tools, and practices of intervention in a longstanding mode of thinking about infrastructures as a security problem (Collier and Lakoff 2008). The related threat discourse consists of an outward-looking focus about non-deterrable threats (in the form of malicious human actors) and an inward looking focus about one's own vulnerability.

The outward-looking focus sees an increasing willingness of malicious actors to exploit weaknesses in an enemy's defense without hesitation or restraint. Government reports are full of references to the cyber-aspect elevating the "old" national security trope to a new urgency-level. This happens through a change in the (interlinked) temporal and the spatial dimension of the threat that make cyber-attack potentially less risky for the aggressor than other type of attacks: In cyberspace, anonymous actors are represented by symbols and their actions unfold their effects anywhere instantaneously—catching them is very difficult or even impossible due to the specificities of the technological environment.

The inward-looking focus on the other hand is about vulnerabilities in (computer) systems. In computer security, a vulnerability is understood as the confluence of three elements that in themselves combine the inward and the outward looking perspective: a system susceptibility or flaw, an attacker's knowledge of and access to the flaw, and an attacker's capability to exploit the flaw (i.e. NIST 2002: 15). The result of a successful utilization of a vulnerability is a compromise of the systems information security. Due to the characteristics of digitally stored information, an intruder can delay, disrupt, corrupt, exploit, destroy, steal, and modify information, with various implications (Waltz 1998).

A general basic issue for cyber-security is that the information infrastructure that we use every day for data-transfer was never built with security in mind: vulnerabilities abound. One of the reasons for the continued existence and constant new creation of these vulnerabilities is that security is constantly "underproduced" in a market dominated by the so-called network effect, under which the benefits of a product increase when the number of users increases, and the "winner takes it all". Quasi-monopolies and time pressures lead to a focus on fast delivery in commercial software development. Quality criteria, like security, play only a minor role (Anderson and Moore 2006). Another reason is that the most powerful actors providing the most important information services today have an interest in keeping them insecure: Big Data is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing

strategies through personalized advertising and prediction of future consumer behaviour (Morozov 2013). Therefore, there is no interest in encrypted (and therefore secure) information exchange. On top of this, the intelligence agencies of this world have the same interest in data that can be easily grabbed (Böhme 2005).

The human in this threat discourse is the weakest link that creates vulnerabilities i.e. through "faulty" software development, or the human is a hapless victim that is exploited by i.e. the actions of cyber-criminals. Through the economic damage that is produced that way, the threat is linked back to the economic security and welfare and often back to national security (Dunn Cavelty and Suter 2012). However, humans are also the prime threat in the archetype/stereotype of the "hacker", individuals with technical superpowers, able to easily pose a sever threat to powerful actors with very limited resources (at least in theory) (Conway 2008; Barnard-Wills and Ashenden 2012).

Vulnerable Critical Objects

The selection of a "referent object" of security is closely interrelated with how the threat is represented. As mentioned, some objects—commonly called infrastructures—and the functions they perform are regarded as 'critical' by the authorities (in the sense of 'vital', 'crucial', 'essential') because their prolonged unavailability harbours the potential for major crisis, both political and social (Burgess 2007). In the mid-1990s, the issue of cyber-security was persuasively interlinked with this topic of "critical infrastructures" and their necessary protection and in the process made into a salient national security issue (PCCIP 1997). Because critical infrastructures combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction (Coward 2009: 408f.) that seeks maximum impact.

One classical goal of (national) security is to throw a "protective or preservative measure […] around a valued subject or object" (Dillon and Lobo-Guerrero 2008: 276). Before this security can unfold, the valued subject/object needs to be identified and also localized in space. In cyber-security linked to critical infrastructure protection, the identification and designation of the protection-worthy is performed following the well-established steps of (technical) risk analysis techniques, which contains both an act of "naming" and an act of prioritizing. At the beginning of such an analysis stands the identification of the assets (including services) that are critical: Criticality is seen as a measure of the consequences associated with the loss or degradation of a particular asset or object. Therefore, criticality needs a reference point: it can only exist in relation to something (pre-)defined as important and normal/desirable (Brunner et al. 2010).

Cyber-security linked to critical infrastructures creates and is implemented in a special type of security environment. Whereas the traditional logic of national security suggests unilateral government action and policy, the policies of cyber-security are inevitably blurred by liberalization, domestic considerations and other policy imperatives (Coaffee and Murakami Wood 2006). The management of infrastructure is in general not (or no longer) the prerogative of government; instead it is based on the logic of the market. While it remains the essential task of a

government to provide the security of society, it has simultaneously become impossible for any government to achieve this by itself. What is at stake is not the body of the state or its borders, "but the conjoined body of public and private-sector networks" (Der Derian and Finkelstein 2008: 102). Therefore, the private sector becomes instrumental in not only helping with the act of "identification" of critical objects, but also more directly in assuring the health of networks and the services provided by them.

Whereas the methodology employed to identify critical assets is very similar in both the public and private sector, the commonalities end when it comes to the protection goals. From the public sector's perspective, criticality is linked to the loss of one or more broad national functions. That set of functions—or protection principles—has expanded over time, beginning with national defense and economic security, to include public health and safety, and then national morale (Kristensen 2008). Through definition of these national functions along the lines of general well-being of a nation and its citizens, the link between critical infrastructure protection and national security is forged. For the state, the goal of protection is the collective well-being represented as a way of liberal life (Anderson 2010)—but, by implication, also the continued function of the state. The relationship between state and infrastructure emerges as an alternative to the image of Abraham Bosse's Leviathan on the frontispiece of Hobbes famous book: Instead of being made up of its citizens, the state is regarded as consisting of the things inside its territory that make life there 'good'; assets that are not directly identified with its citizens, but material assets that give substance (and significance) to the state through being its foundation (Dunn Cavelty and Kristensen 2008).

For the private sector, the reference point varies depending on the business model; in the abstract, however, it is their functioning, or 'business continuity', that is the ultimate protection goal. The reference object for companies, therefore, is themselves. Crucial for the continued performance and effectiveness of many of today's companies that operate as traders of information/knowledge with the help of information/knowledge networks, is protection against loss of information and routine preservation of knowledge. These techniques sever the human mind/body as "'incubator' of this knowledge" from the knowledge itself (Der Derian and Finkelstein 2008: 102), which is given autonomous value over that which becomes replaceable as a result of these practices. In this view, humans become reduced to nodes in the network, needed to ensure the wealth and health of the networks, but not their own health.

National Security versus Human Security in Cyberspace

In cyber-security as currently understood and practised, human beings are seen as victims, as weakest link in the system, as direct threat—but not (or only very indirectly) as beneficiaries of the type of security that states (and companies) want. On the one hand, the neglect of the human element is a direct consequence of a focus on technical systems as targets and technology-based countermeasures in cyber-security. On the other hand, the lack of consideration for "the human" in this

field also seems to be an effect of the issue that human security scholarship has already tackled decades ago: that too much focus on the state and national security tends to crowd out consideration for the individual citizen, with often detrimental effects for security overall (cf. Burgess and Owen 2004). I look at both aspects and their consequences for security below and then turn to the clash between this type of security and human security.

Technical Systems, Political Consequences

A focus on technical objects is not a bad thing per-se. In fact, the type of security that emerges directly from the wish to ensure cyber-security is one that seemingly dodges problematic issues normally associated with security, at least in the first instance. Ultimately, we are looking at the practice of protecting inanimate things; the regulation of machines and their performance. Computers, servers, and the computer-powered infrastructures are non-human objects, which are someone's legitimate property and have a certain (usually undisputed) value for societies. Cyber-security measures thus imagined have little to no bearing on citizens' lives directly. Most importantly, there are no concerns about freedom/security trade-offs, and no civil liberty issues (Buzan et al. 1998). This security does not depend upon the invocation of a state of emergency, but is 'clean' and ultimately, 'good', since everybody seems to benefit from an interruption-free performance of vital systems.

However, this view is inevitably problematized, because these machines cannot be isolated from human life. The image of modern complex critical infrastructures is one in which it becomes futile to try and separate the human from the technological. Technology is not simply a tool that makes life livable: rather, technologies become constitutive of novel forms of 'a complex subjectivity', which is characterized by an inseparable ensemble of material and human elements (Coward 2009: 414). Therefore, even if technologies may appear to regulate objectively and apolitically, there is *always* a connection to a place, to a space, to a space of protection, to values, to life. An even closer look at the seemingly apolitical management of a technical issue with technical means reveals a deeply political nature, because the selection of referent objects as described above always entails a larger argument about protection: Endangered entities are judged to have legitimate claims to protection (while others do not). In other words, this type of security will only provide relief to a valued referent object—not necessarily "the citizen" or humans more generally.

In cyber-security, as argued above, economic imperatives like profit maximization are decisive. It is not a given, then, that cyber-security is a truly public good, understood as security for all. Quite the opposite: the type of security that emerges mainly benefits a few and already powerful entities and has no or even negative effects for the rest. The type of referent object to be protected and by implication, the type of life to be saved, is represented by the uninterrupted flow of information linked to the accumulation of capital and economic growth (Swyngedouw 2007), which in turn is linked to national security. This is at the heart of the cyber-security dilemma, in which the dominant form of security is making large parts of the population arguably less secure. Various security needs are not aligned; and while they do not always have to be, more awareness of the clash between them is needed.

State Power in Cyberspace

Referent objects also reveal a lot about (hidden) power structures. Contrary to the beautiful utopia of cyber-libertarians like Barlow (1996), who saw cyberspace as a serious challenge to traditional state power, the dystopian reality is more like a "feudal power structure" that consolidates power in the hands of the few (Schneier 2012a). Even though the cyber-realm has challenged us to think about power differently, the most power rests with a few IT companies that act with little restraint in their own self-interest, often changing social norms by accident or deliberately, at all times using "the users" to increase their profits. At the same time, states are asserting their power positions rather forcefully (Schneier 2013), mostly in the name of security.

Assertion of state power is linked to the possibility (and desirability) to create *borders* in cyberspace, which results in a changing topology of cyberspace as we know it (Mueller et al. 2013). Prominent concepts like "Cyber-Westphalia" tap into the founding myths of a stable political world order based on state power and invoke images of a delimited and thus defendable and securable place, newly reordered by the state as the real guarantor of security (Demchak and Dombrowski 2011). In this view, held by many government actors, the process of re-establishing state control in cyberspace is inevitable, because security is the most basic need of human beings and seeking security will triumph over other, lesser, inferior needs (such as privacy). Furthermore, the more the issue is presented like a traditional national security issue, the more natural it seems that the keeper of the peace in cyberspace should be the military, and the most relevant concepts are cyber-defense, cyber-deterrence, etc. However, actions by military actors with relation to cyberspace directly fuel the cyber-security dilemma as we have seen.

Of course, there is a certain appeal to a vision in which the unruly, anarchical and dangerous side of cyberspace is kept "outside", and relative security can be established among states. However, this image simplifies complex matters in an unbeneficial way: Not only does inside-outside generally not apply easily to cyberspace, state control also often means control over information flows: Indeed, an increasing number of governments are already controlling what their citizens can and cannot do on the Internet. Totalitarian governments are embracing a growing "cyber-sovereignty" movement to further consolidate their power. But democratic states are doing very similar things: There is more government surveillance, more government censorship, and more government propaganda than ever before (Deibert 2013; Wagner 2014).

When Notions of Security Clash

State controlled borders in cyberspace would in most cases amount to (at least partial) governmental control over information flows. Certainly, this does not mean that all states would start misusing this power, but trust in their benign intent with regards to civil liberties, most notably privacy, has taken a serious hit last year with Edward Snowden's NSA revelations. Most notably, the NSA scandal has focused

attention on the fact that there are direct human security implications arising from mass surveillance in the name of national security.

In this day and age, more and more user or system specific data is up for grabs—for anybody who is interested in it, ranging from business, to criminals, and the intelligence services. While just the extensive data *collection* by companies and intelligence agencies is already cause for concern, the consequences of this for human security becomes fully apparent when the possibilities of its analysis are taken into account. With a relatively simple network analysis, detailed insight into the private lives and relationships of each individual can be gained. More sophisticated methods of calculation are less interested in the present but are geared towards the prediction of future behaviour (and motivations) of people (cf. McCue 2007). Such techniques are already used for targeted advertising, whereby an algorithm defines that if Person X buys this or that product, it is very likely that X is also interested in this or that product. In predictive policing, similar techniques are used to calculate crime hot spots (Perry et al. 2013). A goal of intelligence services is to be able to have advance warning of i.e. radicalization or terrorist behaviour, based on data combination that could look like this: If Person X visit this website and that website, is in contact with this and that person and has this specific motion profile, then it is likely that Person X will commit a terrorist attack in the next 2 years.

From a data protection perspective, these developments are daunting, particularly because the so-called commercialization of data is not done against the wishes of the user, but rather because it seems to make our lives so much more efficient and convenient. Sure, targeted advertising is at best intrusive and does not yet constitute a human security threat. However, much more unpleasant implications of individual risk profiles are already apparent today, with people being excluded from certain services, because aspects of their (private) life does not meet the requirements of a company (Amoore and de Goede 2005). In the future, it is not unlikely that even more unpleasant and more directly political relevant implications arise when democratic rights, such as political resistance or dissidence, are seen as an opportunity for government intervention in the sense of "proactive security" (i.e. at airports).

Add to these developments a fantasy about a version of cyberspace in which crime or even attacks by state actors become impossible or at least very hard. Given that the prime issue for traditional law enforcement methods like punishment or well-proven military tools like deterrence is the "attribution problem" (the difficulty of clearly identifying those initially responsible for a cyber-attack), and given that the attribution problem arises from technological protocols that guarantee a great deal of anonymity for its users, taking away said anonymity, in parts or fully, is sometimes seen as one of the best solutions for a secure internet of the future (cf. CSIS 2008: 61ff.). Here, the clash of different types of security becomes directly visible. From a human and political rights perspective, anonymity is not a threat to security, it is a crucial part of it. An Internet without the attribution problem, which would most likely have a negligible effect on security overall, would introduce a new issue: citizens could be readily identified and punished for their political activities (Zittrain 2011).

That said, the security-implications of current actions by state entities go even further. It has been suspected for a while and is now confirmed that the intelligence services of this world are making cyberspace more insecure *directly*; in order to be able to have more access to data, and in order to prepare for future conflict. It has been revealed that the NSA has bought and exploited so-called zero-day vulnerabilities in current operating systems and hardware to inject NSA malware into numerous strategically opportune points of the Internet infrastructure (Greenwald and MacAskill 2013). As soon as military and intelligence agencies became buyers of so-called zero-day vulnerabilities, prizes have skyrocketed (Miller 2007; Perlroth and Sanger 2013), with several downsides to this: first, exposing these vulnerabilities in order to patch them, as was the norm not so long ago, is becoming less likely. Second, the competition for exclusive possession of such vulnerabilities might even give programmers incentives to deliberately create and then sell them (Schneier 2012b). It is unknown which computer systems have been compromised—but it is known that these backdoors or sleeper programs can be used for different purposes (surveillance, espionage, disruption, etc.) and activated at any time. It also has been revealed that the US government spends large sums of money to crack existing encryption standards—and apparently has also actively exploited and contributed to vulnerabilities in widespread encryption systems (Simonite 2013; Fung 2013; Clarke et al. 2013).

The crux of the matter is that these backdoors reduce the security of the entire system—for everyone. The exploitation of vulnerabilities in computer systems by intelligence agencies and their weakening of encryption standards have the potential to destroy trust and confidence in cyberspace overall. Also, there is no guarantee that the backdoor-makers have full control over them and/or can keep them secret—in other words, they could be identified and exploited by criminal hackers or even "terrorists". Here, state practices not only become a threat for human security: paradoxically, they also become a threat for themselves.

From Problem to Solution: Human-Centric Information Ethics

This article has identified and discussed implications of cyber(-in)-security for human-security concerns, with a main focus on both the representation of the issue as a (security) political problem and the practices of (mainly state) actors based on such representations. The problem with the current system is that security is underproduced, both from a traditional state-focused national security and also from a bottom-up, human security perspective. The reason, so I have argued, is a multi-dimensional and multi-faceted security dilemma, produced by the following interlinked issues:

First, cyber-security is increasingly presented in terms of power-struggles, war-fighting, and military action. This is not an inevitable or "natural" development; rather, it is a matter of choice, or at least a matter of (complicated) political processes that has produced this particular outcome. The result is not more security, however, but less: states spend more and more money on cyber-defense and likely also cyber-offense, which is not leading to more, but less security, as evident by the

flood of official documents lamenting the security-deficit. Second, the type of cyber-security that is produced is based on economic maxims, often without consideration for the particular security-needs of the population. Third, extending a notion of national security based on border control to cyberspace will almost inevitably have an impact on civil liberties, especially on the right to privacy and the freedom of speech. Fourth, cyber-exploitation by intelligence agencies linked to the manipulation of vulnerabilities is directly making cyber-space more insecure. What becomes exceedingly clear from the developments and lessons of the last decade is that we cannot have both: a strategically exploitable cyberspace full of vulnerabilities—and a secure and resilient cyberspace that all the cyber-security policies call for.

At the heart of this challenge is, as so often when human security is implicated, the state (cf. Kerr 2007). On the one hand, state practices are emerging as a major part of the problem, constantly creating more insecurity and in fact also hindering the removal of known insecurities. At the same time, a secure, safe, and open cyberspace is not possible without involvement of the state. How, then, can this dilemma be overcome? Because it is a dilemma extending to more than the state, solutions are not to be found solely in the cooperation *between* states (cf. Booth and Wheeler 2008). Rather, a focus on a common issue of interest for all the stakeholders that are interested in more security is needed. Such a common ground is held by *vulnerabilities*.

If we want a secure and resilient cyberspace, then a strategically exploitable cyberspace full of vulnerabilities has to be actively worked against. This is a compromise that some state actors need to make if they want a type of national security that extends to cyberspace. If such a compromise is not made, then the quest for more national security will always mean less cyber-security, which will always mean less national security because of vulnerabilities in critical infrastructures. The reason why vulnerabilities persist and even proliferate has already been identified above: the current incentive structures in the market are skewed (Dynes et al. 2008). This is where states are needed to help improve cyber-security through additional regulation (and through further encouragement of voluntary arrangement for the increase of cyber-security in the corporate sector). Furthermore, there is no doubt from a human security perspective that the zero-day exploit "market" needs to be regulated internationally for security reasons (Kuehn 2013). In addition, prime human security concerns like the freedom of speech and the right to privacy should no longer be seen as anti-security, but as *pro*-security if linked to vulnerabilities: reducing the amount of data that is unencrypted will substantially reduce cyber-crime and cyber-espionage, with benefits for both human-centred and state-centred security.

In turn, the ethics that should guide our future engagement with cyber-security have to take into account the special and all-embracing characteristics of cyberspace. So far, ethical considerations with bearing on cyber-security have mainly been made from a military perspective, following the tradition to address new forms of warfare and weapons systems under ethical viewpoints (cf. Rowe 2010; Dipert 2010; Barrett 2013). Cyber-security, as argued in the very beginning, is far more than this, however: From both a state and a human security perspective,

cyberspace has become more than just a technological realm in which we sometimes interact for social or economic reasons. Cyberspace has become a fundamental part of life and is constitutive of new, complex subjectivities.

An ethics that fits such a broad understanding is *Information Ethics*. It constitutes an expansion of environmental ethics towards a less anthropocentric concept of agent, which includes non-human (artificial) and non-individual (distributed) entities and advances a less biologically-centred concept of "patient", which includes not only human life or simply life, but any form of existence. This ethics is concerned with the question of an "ethics in the infosphere" (Floridi 2001) and beyond that, an "ethics *of* the infosphere" (Capurro 2006). In information ethics, the lowest possible common set of attributes which characterises something as intrinsically valuable and an object of respect is its abstract nature as an informational entity (Floridi 1998). In this view, all informational objects are in principle worth of ethical consideration. However, to ensure that such an ethics does not involuntarily place the technical over the social, we must make sure that the protection of these data is not founded "on the dignity of the digital but on the human dimensions they refer to" (Capurro 2006). The duty of a moral agent is evaluated in terms of contribution to the growth and welfare of the entire infosphere (Floridi 1999: 47), but always related to a bodily being in the world. Any process, action or event that negatively affects the infosphere with relevance to human life impoverishes it and is an "instance of evil" (Floridi and Sanders 1999, 2001). Vulnerabilities are such an evil.

References

Amoore, L., & De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change, 43*(2–3), 149–173.

Anderson, B. (2010). Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography, 34*(6), 777–798.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*, 610–623.

Axworthy, L. (2001). Human security and global governance: Putting people first. *Global Governance, 7*(1), 19–24.

Barlow, J. P. (1996). A declaration of the independence of cyberspace, electronic frontier foundation website. http://homes.eff.org/~barlow/Declaration-Final.html.

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture, 15*(2), 110–123.

Barrett, E. T. (2013). Warfare in a new domain: The ethics of military cyber-operations. *Journal of Military Ethics, 12*(1), 4–17.

Böhme, R. (2005). Vulnerability markets—What is the economic value of a zero-day exploit? Paper held at the 2005 Chaos Communication Congress Berlin, Germany. http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf.

Booth, K., & Wheeler, N. (2008). *The security dilemma: Fear, cooperation and trust in world politics*. New York: Palgrave.

Boulanin, V. (2013). Cybersecurity and the arms industry. *SIPRI Yearbook 2013: Armaments, disarmament and international security* (pp. 218–226). Oxford: Oxford University Press.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center George Mason University, Working Paper No. 11-24, April 2011.

Brunner, E., Dunn Cavelty, M., Giroux, J., & Suter, M. (2010). Protection goals. Focal report on Critical Infrastructure Protection for the Federal Office for Civil Protection, No. 4. Zurich: Center for Security Studies.

Burgess, J. P. (2007). Social values and material threat: The European Programme for Critical Infrastructure Protection. *International Journal of Critical Infrastructures, 3*(3–4), 471–487.

Burgess, J. P. & Owen, T. (Eds.) (2004). Special section: What is 'human security'?, *Security Dialogue*, 35(3), 345–346.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.

Capurro, R. (2006). Towards an ontological foundation of information ethics. *Ethics and Information Technology, 8*(4), 175–186.

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., & Swire, P. (2013). Liberty and security in a changing world: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Washington, DC. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Coaffee, J., & Murakami Wood, D. (2006). Security is coming home: Rethinking scale and constructing resilience in the global urban response to terrorist risk. *International Relations, 20*(4), 503–517.

Collier, S. J. & Lakoff, A. (2008). The vulnerability of vital systems: How critical infrastructure became a security problem. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *The politics of securing the homeland: Critical infrastructure, risk and securitization* (pp. 17–39). New York: Routledge.

Conway, M. (2008). The media and cyberterrorism: A study in the construction of 'reality. In M. Dunn Cavelty & K.S. Kristensen (Eds.), *The politics of securing the homeland: Critical infrastructure, risk and securitisation* (pp. 109–129). London: Routledge.

Coward, M. (2009). Network-centric violence, critical infrastructure and the urbanization of security. *Security Dialogue, 40*(4–5), 399–418.

CSIS Center for Strategic and International Studies (2008). Securing Cyberspace for the 44th Presidency A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. Toronto: McClelland & Stewart.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2008). *The practice and policy of global internet filtering*. Cambridge: MIT Press.

Demchak, C. & Dombrowski, P. (2011). Rise of a cybered westphalian age. Strategic Studies Quarterly, Spring, pp. 32–61.

Der Derian, J. & Finkelstein, J. (2008). Critical infrastructures and network pathologies: The semiotics and biopolitics of heteropolarity. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *The politics of securing the homeland: critical infrastructure, risk and securitisation* (pp. 84–105). London: Routledge.

Dillon, M., & Lobo-Guerrero, L. (2008). Biopolitics of security in the 21st century: An introduction. *Review of International Studies, 34*(2), 265–292.

Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics, 9*(4), 384–410.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.

Dunn Cavelty, M. (2012). Militarizing cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *Proceedings of the 4th International Conference on cyber conflict* (pp. 141–153). Tallinn: CCD COE Publications.

Dunn Cavelty, M. & Kristensen, K.S. (2008). Introduction: Securing the homeland: Critical infrastructure, risk, and (in)security. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *The politics of securing the homeland: Critical infrastructure, risk and securitization* (pp. 1–14). New York: Routledge.

Dunn Cavelty, M. & Suter, M. (2012). The art of CIIP strategy: Taking stock of content and processes. In J. Lopez, R. Setola, S. D. Wolthusen (Eds.). Critical infrastructure protection: Information infrastructure models, analysis, and defense (pp. 15–38). Springer: Berlin.

Dynes, S., Goetz, E., & Freeman, M. (2008). Cyber Security: Are economic incentives adequate? In E. Goetz & S. Shenoi (Eds.), *Critical infrastructure protection, IFIP International Federation for Information Processing* (Vol. 253, pp. 15–27). Boston: Springer.

Floridi, L. (1998). Does information have a moral worth in itself? Paper presented at Computer Ethics: Philosophical Enquiry in Association with the ACM SIG on Computers and Society, London School of Economics and Political Science, London, December 14–15, 1998. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=144548.

Floridi, L. (1999). Information ethics: On the theoretical foundations of computer ethics. *Ethics and Information Technology, 1*(1), 37–56.
Floridi, L. (2001). Ethics in the Infosphere. *The Philosophers' Magazine, 6*, 18–19.
Floridi, L. & Sanders, J. W. (1999). Entropy as evil in information ethics. *Etica & Politica*, special issue on Computer Ethics, 1(2).
Floridi, L., & Sanders, J. W. (2001). Artificial evil and the foundation of computer ethics. *Ethics and Information Technology, 3*(1), 55–66.
Fung, B. (2013). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. Washington Post. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-bybuying-millions-of-dollars-worth-of-computer-vulnerabilities/.
Greenwald, G. & MacAskill, E. (2013). Obama orders US to draw up overseas target list for cyber-attacks, The Guardian. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.
Hagmann, J., & Dunn Cavelty, M. (2012). National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue, 43*(1), 80–97.
Hoogensen, G., & Stuvøy, K. (2006). Gender, resistance and human security. *Security Dialogue, 37*(2), 207–228.
Jervis, R. (1978). Cooperation under the security dilemma. *World Politics, 30*(2), 167–214.
Kerr, P. (2007). Human security. In A. Collins (Ed.), *Contemporary security studies* (pp. 122–134). Oxford: Oxford University Press.
Kristensen, K.S. (2008). The absolute protection of our citizens: Critical infrastructure protection and the practice of security. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *The politics of securing the homeland: Critical infrastructure, risk and securitisation* (pp. 63–83). London: Routledge.
Kuehn, A. (2013). Extending cybersecurity, securing private internet infrastructure: The U.S. Einstein Program and its Implications for Internet Governance. In R. Radu, J.-M. Chenou & R.H. Weber (Eds.) *The evolution of global internet governance* (pp. 157–167). Schulthess: Zürich.
McCue, C. (2007). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Oxford: Butterworth Heinemann.
Miller, C. (2007). The legitimate vulnerability market: The secretive world of 0-day exploit sales. In 6th Workshop on the Economics of Information Security (WEIS 2007). http://weis2007.econinfosec.org/papers/29.pdf.
Morozov, E. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist*. London: Allen Lane.
Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review, 15*(19), 86–104.
NIST (2002). NIST Special Publication 800-30, Risk Management Guide for Information Security.
PCCIP President's Commission on Critical Infrastructure Protection. (1997). *Critical foundations: Protecting America's infrastructures*. Washington: US Government Printing Office.
Perlroth, N., & Sanger, D. E. (2013). Nations buying as hackers sell knowledge of software flaws. *The New York Times, 14*, A1.
Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND.
Rowe, N. C. (2010). The ethics of cyberweapons in warfare. *International Journal of Techoethics, 1*(1), 20–31.
Rueter, N. (2011). The Cybersecurity Dilemma. MA thesis. Duke University.
Schneier, B. (2012a). The vulnerabilities market and the future of security. Forbes, May 30. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-ofsecurity/.
Schneier, B. (2012b). When it comes to security, we're back to Feudalism. Wired, http://www.wired.com/opinion/2012/11/feudal-security/.
Schneier, B. (2013). The battle for power on the internet. The Atlantic, http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824.
Simonite, T. (2013). NSA's own hardware backdoors may still be a "problem from hell", http://www.technologyreview.com/news/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/.
Stevens, T., & Betz, D. J. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147–164.

Swyngedouw, E. (2007). Impossible/undesirable sustainability and the post-political condition. In J. R. Krueger & D. Gibbs (Eds.), *The sustainable development paradox* (pp. 13–40). New York: Guilford Press.

Wagner, B. (2014). The politics of internet filtering: The United Kingdom and Germany in a comparative perspective. *Politics, 34*(1), 58–71.

Waltz, E. (1998). *Information warfare: Principles and operations*. Boston: Artech House.

Zittrain, J. (2011). Freedom and anonymity: Keeping the internet open, http://www.scientificamerican.com/article/freedom-and-anonymity/.